CLAIMS

1. Method for establishing security in an ad hoc communication network (106), the ad hoc network (106) comprising a set of communication nodes (101, 103-105) whereof at least two of the nodes (103-105) having a mutual trust relation and thus constituting a trust group (102), the trust relations being created with public keys, and at least one additional node (101), being a candidate for joining the trust group (102) within the ad hoc network (106), **characterised** by the nodes having authority to delegate trust to nodes they trust,
the method comprising the steps of
   - a) identifying a node (103) within the trust group having a trust relation with the candidate node (101), a so-called X-node (103);
   - b) distributing trust relations between all the members in the trust group (102) and the candidate node (101) by means of the X-node (103).

2. The method of claim 1, **characterised** by comprising the further step to be taken before step a), the candidate node (101) sending a message, comprising its public key, to all nodes (103-105) within the network.

3. The method of any of the previous claims, **characterised** in that the ad hoc network (106) comprises a single trust group (102), and a single candidate node (101), wherein step b), implies that the X-node (103) sends a signed message, comprising a list of the nodes (104, 105) that the X-node (103) trusts within the ad hoc network (106), and all their corresponding public keys, to the candidate node (101).

4. The method according to any of the previous claims, **characterised** in that step b) further implies that the X-node (103) signs the candidate node's (101) public key.

5. The method according to the previous claim, **characterised** in that step b) further implies, the X-node (103), sends a message, comprising the candidate node's (101) signed public key, to the nodes (104-105) within the trust group (102).

6. The method according to claim 2 **characterised** in that the ad hoc network (201) comprises a set of nodes (A-M) comprising several trust groups (202-205), and all nodes (A-M) being candidates for joining all trust groups, within the ad hoc network, that they are not already a member of, the method comprising the further step to be taken, by each node (A-M), after receiving the messages from all candidate nodes (A-M),
creating a list of the candidate nodes that the particular node trusts and their corresponding public keys.

7. The method according to the previous claim, **characterised** by further comprising the step of deciding one node (A) within the ad hoc network (201) to act as a server node (A).

8. The method according to any of the claims 6-7, **characterised** by further comprising the step of, the server node (A) receiving from each other node (B-M) within the network, a message comprising its respective public key, the respective list of the candidate nodes that the respective node trust and their corresponding public keys.

9. The method according to the previous claim, **characterised** by further comprising the step of, the server node (A) *classifying* the at least one candidate node as being a server-trusted node (B, C, D, E, F and I) or as being a server-untrusted node (G, H, J, K, L and M), depending on whether the server node (A) trusts it or not.

10. The method according to the previous claim, wherein a server-trusted node trusting a server-untrusted node constitutes a so-called Y-node, **characterised** in that the step a) implies that the server node (A) identifies at least one Y-node required for distributing trust relations between the server node (A) and as many server-untrusted nodes as possible.

11. The method according to the previous claim, **characterised** in step b) further implying that server node (A) sends a request to the identified Y-nodes (D, H) of distributing said trust relations between server node A and server-untrusted nodes.

12. The method according to the previous claim, **characterised** in step b) further implying that server node (A) obtains said requested trust relations.

13. The method according to the previous claim, **characterised** in, the step of obtaining the trust relations comprising that for each server-untrusted node that the Y-node have a trust relation with, the Y-node signs the public key of the server node (A) and forwards it to the server-untrusted node.

14. The method according to any of the claims 12-13, **characterised** in the step of obtaining the trust relations comprising that for each server-untrusted node that the Y-node have a trust relation with, the Y-node signs the public key of the server-untrusted node and forwards it to the server node (A).

15. The method according to any of the claims 12-14, **characterised** by comprising the further step of, server node (A), after obtaining said trust relation, reclassifying the server-untrusted node with the obtained trust relation as being a server-trusted node.

16. The method according to any of the claims 12-15, **characterised** by comprising the further step of, server node (A) sending a signed message comprising the server node's (A) all trusted public keys belonging to trusted candidate nodes within the ad hoc network. (201).

17. An ad hoc communication network (106) comprising a set of communication nodes (101, 103-105) whereof

the nodes (101, 103-105) each comprising a receiver and a computer, the computer comprising a processor and a memory,

the nodes (101, 103-105) being interconnected with communication links,

at least two of the nodes (103-105) are having a mutual trust relation and thus constituting a trust group (102), the trust relations being created with public keys, and

at least one additional node (101) being a candidate for joining at least one trust group (102) within the ad hoc network,

characterised by

the candidate node (101) having means for requesting if any of the nodes within the trust group (102) have a trust relation with the candidate node (101),

the nodes being authorised to and are having means for, distributing trust relations between its trust group(102) and the candidate node (101) that it trusts.

18. The ad hoc communication network (201) according to the previous claim, **characterised** by each node (A-M) having means for creating a list of the candidate nodes that the node trusts and their corresponding public keys, to be stored in the memory.

19. The ad hoc communication network according to any of the claims 17-18, **characterised** in that one node (A) within the ad hoc network (201) being a server node (A), capable of administrate distribution of trust relations.

20. The ad hoc communication network (201) according to the previous claim, characterised by the server node (A) having means for classifying the at least one candidate node as being a server-trusted node (B, C, D, E, F and I), or as being a server-untrusted node (G, H, J, K, L and M), depending on whether the server node (A) trusts the candidate node or not.

21. The ad hoc communication network (201) according to the previous claim, wherein a server-trusted node trusting a server-untrusted node constitutes a so-called Y-node characterised by the server node (A) having means for identifying at least one Y-node (D, H) required for distributing trust relations between the server node A and the server-untrusted nodes.

22. The ad hoc communication network (201) according to the previous claim characterised by the server node (A) having means for sending to each of the identified Y-nodes (D, H),

a request as to which of the server-untrusted nodes (G, H, J and M) the Y-node (D, H) has a trust relation with, and

a request for distributing trust relations between the server node (A) and the requested server-untrusted nodes.

23. The ad hoc communication network according to any of the claims 20-22, characterised by the server node (A) having means for distributing obtained trust relations to the nodes within the ad hoc communication network (201).

24. A computer program product directly loadable into the internal memory of a digital computer within a node being a member of an ad hoc communication network, comprising software code portions for performing the steps of any of the claims 1-16 when said product is run on a computer.

25. A computer program product stored on a computer usable medium, comprising readable program for causing a computer, within a node being a member of an ad hoc communication network, to control an execution of the steps of any of the claims 1-16.